Vulnerabilidad de Cross-Site Scripting (XSS) Reflejado en el campo de búsqueda.

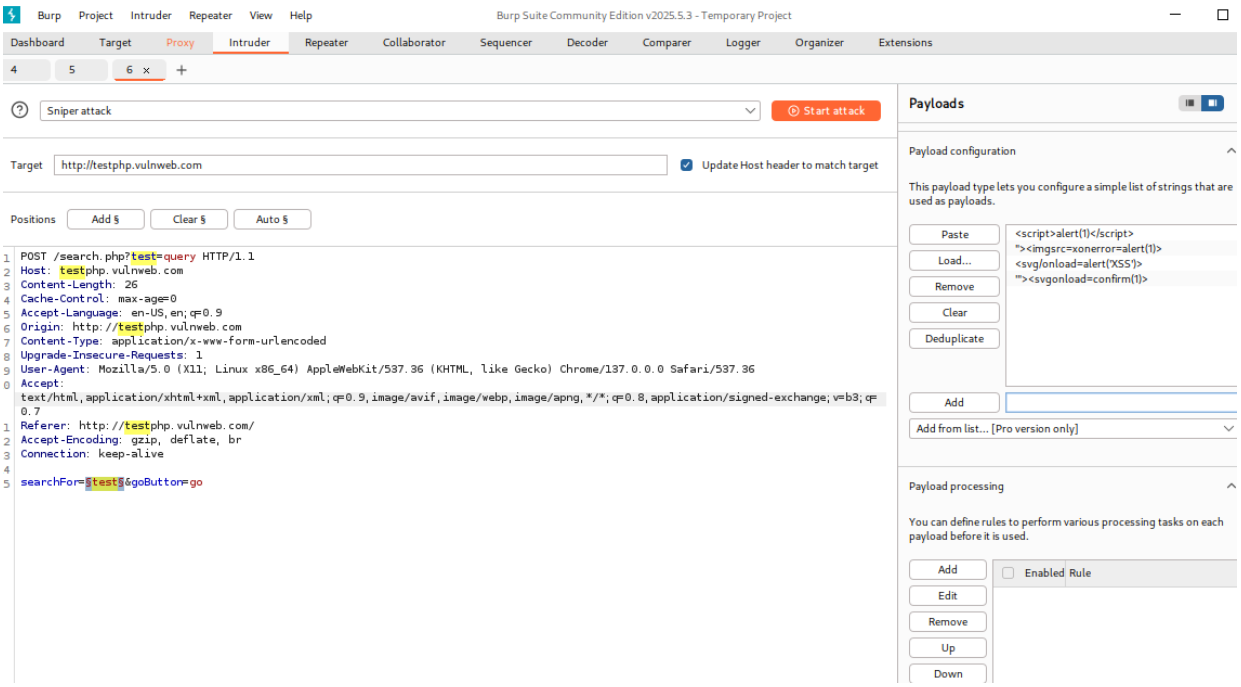
Descripción

Se detectó una vulnerabilidad de XSS reflejado en el formulario de búsqueda de la aplicación web. El campo de búsqueda no valida ni sanitiza adecuadamente la entrada del usuario, permitiendo la inyección de código JavaScript que se ejecuta en el navegador del usuario final.

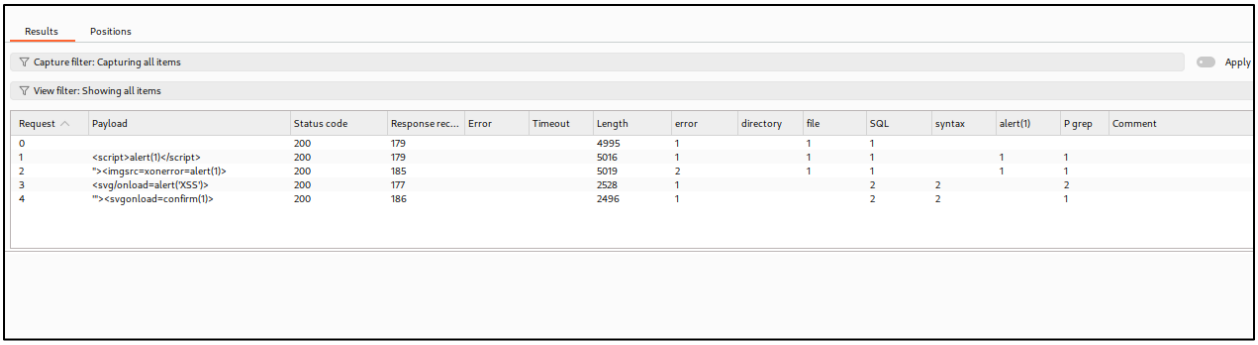
Evidencia Técnica

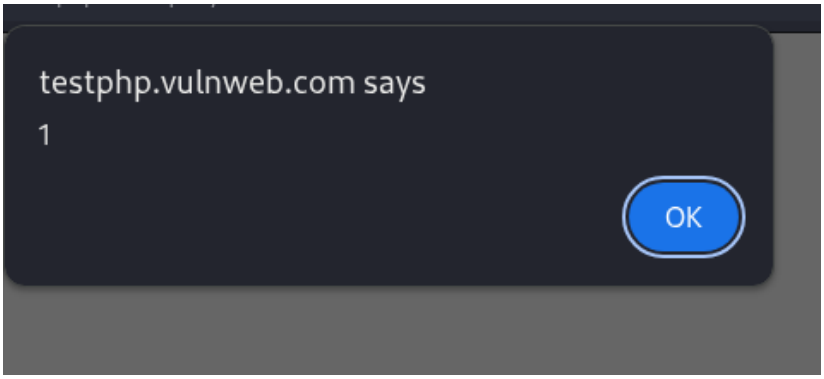
La vulnerabilidad fue detectada mediante la técnica de **fuzzing** automatizado con la herramienta **Burp Suite**.

- **Payloads utilizados**: Se inyectaron varios payloads maliciosos, incluyendo <script>alert(1)</script>.



- **Comportamiento del sistema**: El servidor devolvió una respuesta que reflejaba el código malicioso en la página HTML, lo que indica que no se implementó un filtrado de entrada adecuado. El uso del **Grep** de Burp Suite lo confirmó al encontrar la cadena alert(1) en la respuesta, como se muestra en la siguiente captura de pantalla.





Evaluación de Impacto y Riesgo

- **Impacto**: Alto. Una explotación exitosa podría permitir a un atacante robar cookies de sesión, secuestrar la cuenta del usuario, redirigir a los usuarios a sitios maliciosos o realizar ataques de phishing.
- **Riesgo**: Alto. La vulnerabilidad es fácil de explotar y su impacto potencial es significativo, comprometiendo la confidencialidad y la integridad de los datos de los usuarios.

Recomendaciones Técnicas

- **Validación de Entrada**: Implementar una validación estricta de la entrada en el servidor, utilizando una lista blanca de caracteres permitidos y rechazando cualquier código HTML o JavaScript.
- **Codificación de Salida (Output Encoding)**: Asegurar que todo el contenido generado por el usuario que se muestre en la página esté correctamente codificado para que el navegador lo interprete como texto plano y no como código ejecutable.
- **Content Security Policy (CSP)**: Implementar una política de seguridad de contenido para restringir las fuentes desde las que se pueden cargar scripts y otros recursos, mitigando la ejecución de código no autorizado.

Reflexión Final

- **¿Cómo se diferencia un informe profesional de una simple alerta técnica?** Un informe profesional va más allá de solo identificar un fallo. Describe la vulnerabilidad, muestra evidencia reproducible, analiza el riesgo real y propone soluciones concretas. Usa un lenguaje claro y estructurado, lo que lo hace accionable para los equipos de desarrollo y comprensible para la gerencia, facilitando la toma de decisiones informadas.
- **¿Qué aprendiste sobre la importancia del lenguaje y la estructura en un reporte de seguridad?** La estructura y el lenguaje son fundamentales para el impacto del informe. Un reporte bien organizado con un lenguaje preciso y sin ambigüedades asegura que el equipo de desarrollo entienda el problema, los riesgos y las soluciones propuestas, mejorando la respuesta a la vulnerabilidad.